

EFFECTIVE RESULTS ON LINEAR DEPENDENCE FOR ELLIPTIC CURVES

MIN SHA AND IGOR E. SHPARLINSKI

ABSTRACT. Given a subgroup Γ of rational points on an elliptic curve E over \mathbb{Q} of rank $r \geq 1$ and a sufficiently large real $x \geq 2$, suppose that the rank of Γ is less than r , then we give unconditional and conditional upper and lower bounds on the canonical height of a rational point Q which is not in the group Γ but belongs to the reduction of Γ modulo every prime $p \leq x$ of good reduction.

1. INTRODUCTION

1.1. Background and motivation. Let A be an Abelian variety defined over a number field F , and let Λ be a subgroup of the Mordell-Weil group $A(F)$. For any prime \mathfrak{p} (of F) of good reduction, we denote by $\Lambda_{\mathfrak{p}}$ the image of Λ via the reduction map modulo \mathfrak{p} , and $F_{\mathfrak{p}}$ stands for the residue field of F modulo \mathfrak{p} . The following question was initiated in 2002 and was considered at the same time but independently by Gajda (in a letter to Kenneth Ribet in 2002, see [9]) and Kowalski [15], and it is now called *detecting linear dependence*.

Question 1. *Suppose that P is a point of $A(F)$ such that for all but finitely many primes \mathfrak{p} of F , as a point in $A(F_{\mathfrak{p}})$, we have $P \in \Lambda_{\mathfrak{p}}$. Does it then follow that $P \in \Lambda$?*

An early result related to this question is due to Schinzel [26], who has answered affirmatively the question for the multiplicative group in place of an Abelian variety. Question 1 has been extensively studied in recent years and much progress has been made; see [5, 6, 7, 9, 12, 13, 20, 23, 31] for more details and developments. For example, Kowalski [15] has shown that the property in Question 1 holds for an elliptic curve and a cyclic subgroup, and Banaszak, Gajda and Krasoń [6] have established such a property for elliptic curves without complex multiplications and a finitely generated free subgroup. In particular, Jossen [12] has given an affirmative answer when A is a simple Abelian

2010 *Mathematics Subject Classification.* 11G05, 11G50.

Key words and phrases. Elliptic curve, linear dependence, pseudolinearly dependent point, pseudomultiple, canonical height.

variety, which automatically includes elliptic curves, in a stronger form that we only need “for a set of primes \mathfrak{p} with natural density 1” instead of “for all but finitely many primes \mathfrak{p} ”. We remark that the answer of Question 1 is not always positive; see [13] for a counterexample.

Here, motivated by Question 1 and in some sense, we introduce and study its counterpart, called *pseudolinear dependence*, in the case of elliptic curves. Following the set up of [1], which is crucial for some of our approaches, we restrict ourselves to the case of elliptic curves over the rational numbers, see Definitions 2 and 3 below. There is little doubt that one can extend [1], and thus our results to elliptic curves over number fields, but this may require quite significant efforts. A result of Banaszak and Krasoń [7, Theorem 7.7] replaces the condition of linear dependence modulo all but finitely many primes by the linear dependence modulo a finite set of primes depending on all the initial data (including the point P), and then recently Sadek [23] has given an explicit upper bound of such primes in the set for a specific class of elliptic curves under the *Generalised Riemann Hypothesis* (GRH). In fact, all results that are based on the Chebotarev Density Theorem involve only a finite set of primes depending on the initial data; see also [9]. Here, using some new ideas, we show that any set of primes that detects the linear dependence should contain large primes; see Theorems 4, 5 and 6 below for more details.

We first fix some notation.

Let E be an elliptic curve over \mathbb{Q} of rank r and of discriminant Δ_E . We denote by $E(\mathbb{Q})$ the Mordell-Weil group of rational points on E . We also let Γ be a subgroup of $E(\mathbb{Q})$ with rank s . We refer to [29] for a background on elliptic curves.

Similarly, for a prime p of good reduction (that is, $p \nmid \Delta_E$), we let $E(\mathbb{F}_p)$ be the group of \mathbb{F}_p -points in the reduction of E to the finite field \mathbb{F}_p of p elements.

We also denote by Γ_p the reduction of Γ modulo p , which is a subgroup of $E(\mathbb{F}_p)$. In particular, $E(\mathbb{Q})_p$ stands for the reduction of $E(\mathbb{Q})$ modulo p .

Definition 2 (\mathbb{F}_p -pseudolinear dependence). *Given a prime p of good reduction, we call a point $Q \in E(\mathbb{Q})$ an \mathbb{F}_p -pseudolinearly dependent point of Γ if $Q \notin \Gamma$ but as a point in $E(\mathbb{F}_p)$ we have $Q \in \Gamma_p$.*

We remark that the \mathbb{F}_p -pseudolinear dependence equivalently means that such a point $Q \notin \Gamma$ but $Q \in \Gamma + \ker_p$, where \ker_p denotes the kernel of the reduction map modulo p .

Definition 3 (x -pseudolinear dependence). *We say that a point $Q \in E(\mathbb{Q})$ is an x -pseudolinearly dependent point of Γ if $Q \notin \Gamma$ but it is*

an \mathbb{F}_p -pseudolinearly dependent point of Γ for all primes $p \leq x$ of good reduction.

In particular, if Γ is generated by a point P , we also say that such a point Q is an x -pseudomultiple of P . This notion is an elliptic analogue of the notions of x -pseudosquares and x -pseudopowers over the integers, which dates back to the classical results of Schinzel [24, 25, 27] and has recently been studied in [3, 8, 14, 21].

In this paper, we explicitly construct such an x -pseudolinearly dependent point Q of Γ provided that $s < r$ and give upper bounds for its canonical height, and then we also deduce lower bounds for the height of any x -pseudolinearly dependent point in some special cases.

More detailedly, we first briefly consider the existence problem of x -pseudolinearly dependent points. Further, essentially using a result of Gupta and Murty [10, Lemma 14], we obtain an unconditional upper bound on the height of an x -pseudolinearly dependent point of Γ if $s < r$. Then, using a result of Akbary, Ghioca and Murty [1, Theorem 1.2] and under GRH we obtain a stronger conditional upper bound provided that $s \geq 19$ if E is a non-CM curve, or $s \geq 7$ if E is a CM curve. In addition, following some detailed theory on the number fields generated by some points of E and applying the effective Chebotarev Density Theorem, we establish unconditional and conditional lower bounds for the height of such points in some special cases.

In the last section, we pose some problems which may merit further study.

1.2. General notation. Throughout the paper, we use the Landau symbols O and o and the Vinogradov symbol \ll (sometimes written as \gg). We recall that the assertions $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \leq cV$ with some absolute constant c , while $U = o(V)$ means that $U/V \rightarrow 0$. In this paper, the constants implied in the symbols O and \ll depend only possibly on E and Γ .

The letter p , with or without subscripts, always denotes a prime. As usual, $\pi(x)$ denotes the number of primes not exceeding x .

We use \hat{h} to denote the canonical height of points on E , see Section 3.2 for a precise definition. For a finite set S , we use $\#S$ to denote its cardinality.

1.3. Main results. Here, we let E be an elliptic curve of rank r defined over \mathbb{Q} , and Γ a subgroup of $E(\mathbb{Q})$ with rank s .

We first state several upper bounds for the height of pseudolinearly dependent points.

Theorem 4. *Suppose that $r \geq 1$ and $s = 0$. Then for a sufficiently large x , there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \leq \exp \left(2x - 2 \log(\#\Gamma) \frac{x}{\log x} + O(x/(\log x)^2) \right)$$

such that Q is an x -pseudolinearly dependent point of Γ .

Theorem 5. *Assume that $r \geq 2$ and $1 \leq s < r$. Then for a sufficiently large x , there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \leq \exp \left(\frac{4}{s+2}x + O(x/\log x) \right)$$

such that Q is an x -pseudolinearly dependent point of Γ .

Theorem 6. *Suppose that either $19 \leq s < r$ if E is a non-CM curve, or $7 \leq s < r$ if E is a CM curve. Then under GRH and for a sufficiently large x , there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \leq \exp (4x(\log \log x)/\log x + O(x/\log x))$$

such that Q is an x -pseudolinearly dependent point of Γ .

Notice that by Definition 3 the condition for x -pseudolinearly dependent points of Γ is quite strong when x tends to infinity. This convinces us that there maybe exist some lower bounds for the height of such points. Here, we establish some partial results.

Theorem 7. *Suppose that $r \geq 1$ and $s = 0$. Then for any sufficiently large x and any x -pseudolinearly dependent point Q of Γ , we have*

$$\hat{h}(Q) \geq \frac{1}{\#\Gamma}x/\log x + O(x/(\log x)^2).$$

Theorem 8. *Assume that $r \geq 2$, $1 \leq s < r$, and Γ is a free subgroup of $E(\mathbb{Q})$. Then for any sufficiently large x and any x -pseudolinearly dependent point Q of Γ , we have*

$$\hat{h}(Q) \geq \exp \left((\log x)^{1/(2s+6)+o(1)} \right);$$

and furthermore assuming GRH, we have

$$\hat{h}(Q) \geq \exp \left(x^{1/(4s+12)+o(1)} \right).$$

2. PRELIMINARIES

2.1. Jossen's result. We want to highlight the following result which is implied in the main theorem of Jossen [12]. As mentioned before, the original result is about simple Abelian varieties over number fields.

Lemma 9. *Let E be an elliptic curve over \mathbb{Q} , and let Γ be a subgroup of $E(\mathbb{Q})$ and $Q \in E(\mathbb{Q})$ a rational point. If the set of primes p for which $Q \in \Gamma_p$ has asymptotic natural density 1, then $Q \in \Gamma$.*

2.2. Heights on elliptic curves. We recall briefly the definitions and relation of the Weil height and the canonical height of points in $E(\mathbb{Q})$; see [29, Chapter VIII, Section 9] for more details.

For a point $P = (x, y) \in E(\mathbb{Q})$ with $x = a/b$, a and b are coprime integers, we define the Weil height of P as

$$\mathfrak{h}(P) = \log \max\{|a|, |b|\},$$

and the canonical height of P is defined as

$$\hat{h}(P) = \lim_{n \rightarrow +\infty} \frac{\mathfrak{h}(2^n P)}{4^n}.$$

These two heights are related by the following:

$$\hat{h}(P) = \mathfrak{h}(P) + O(1),$$

where the implied constant depends only on E . In addition, for any $P \in E(\mathbb{Q})$ and $m \in \mathbb{Z}$, we have

$$\hat{h}(mP) = m^2 \hat{h}(P);$$

furthermore, $\hat{h}(P) = 0$ if and only if P is a torsion point.

2.3. Two useful facts about elliptic curves. First, for any prime p of good reduction, the reduction map modulo p from $E(\mathbb{Q})$ to $E(\mathbb{F}_p)$ is injective when restricted to the torsion subgroup; see [29, Chapter VII, Proposition 3.1]. Hence, if $E(\mathbb{Q})$ has rank 0, then there is no \mathbb{F}_p -pseudolinear dependence, and thus there is no x -pseudolinear dependence in $E(\mathbb{Q})$.

Second, every rational point P in $E(\mathbb{Q})$ has a representation of the form

$$(1) \quad P = \left(\frac{m}{k^2}, \frac{n}{k^3} \right),$$

where m, n and k are integers with $k \geq 1$ and $\gcd(m, k) = \gcd(n, k) = 1$; see [30, page 68]. So, for any prime p of good reduction, $P \equiv O_E$ modulo p if and only if $p \mid k$. In particular, given a point $P \in E(\mathbb{Q})$, there are only finitely many primes p such that $P \equiv O_E$ modulo p .

From the above fact, it is easy to see that if $E(\mathbb{Q}) \neq \{O_E\}$, then there are at most finitely many primes p of good reduction such that $E(\mathbb{Q})_p = \{O_E\}$. This let our definitions and considerations make sense.

Indeed, if $E(\mathbb{Q})$ has more than one torsion point, then by the injectivity of the reduction map restricted to the torsion subgroup, we know that $E(\mathbb{Q})_p \neq \{O_E\}$ for any prime p of good reduction. Otherwise if

$E(\mathbb{Q})$ is a free abelian group of rank r generated by P_1, \dots, P_r , then by the above discussion there exists a prime ℓ such that for any prime $p > \ell$ of good reduction, at least one P_i ($1 \leq i \leq r$) satisfies $P_i \not\equiv O_E$ modulo p , that is $E(\mathbb{Q})_p \neq \{O_E\}$.

2.4. Number fields derived from elliptic curves. Following [1, 10, 19], we recall some basic facts about the number fields generated by division points and points of infinite order on E . Here, we should assume that $E(\mathbb{Q})$ is of rank $r \geq 1$.

Let ℓ be a prime, and $P_1, P_2, \dots, P_n \in E(\mathbb{Q})$ independent points of infinite order on E . Consider the number field

$$L = \mathbb{Q}(E[\ell], \ell^{-1}P_1, \dots, \ell^{-1}P_n),$$

where $E[\ell]$ is the set of ℓ -torsion points on E , and each $\ell^{-1}P_i$ ($1 \leq i \leq n$) is a fixed point whose multiplication by ℓ is the point P_i . Moreover, we denote $K = \mathbb{Q}(E[\ell])$ and $K_i = \mathbb{Q}(E[\ell], \ell^{-1}P_i)$ for every $1 \leq i \leq n$.

Now, both the extensions K/\mathbb{Q} and L/\mathbb{Q} are Galois extensions. For the Galois groups, $\text{Gal}(K/\mathbb{Q})$ is a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$, $\text{Gal}(L/K)$ is a subgroup of $E[\ell]^n$, and $\text{Gal}(L/\mathbb{Q})$ is a subgroup of the semi-direct product

$$\text{GL}_2(\mathbb{F}_\ell) \ltimes E[\ell]^n,$$

which implies that for any $i \neq j$ with $1 \leq i, j \leq n$, we have $K_i \cap K_j = K$. In particular, we have

$$(2) \quad [K : \mathbb{Q}] < \ell^4 \quad \text{and} \quad [L : K] \leq \ell^{2n}.$$

Furthermore, Ribet [22] has shown that for sufficiently large ℓ , the Galois group $\text{Gal}(L/K)$ is isomorphic to $E[\ell]^n$ via the map

$$(\ell^{-1}P_1, \dots, \ell^{-1}P_n) \mapsto (\ell^{-1}P_1 + A_1, \dots, \ell^{-1}P_n + A_n),$$

where $(A_1, \dots, A_n) \in E[\ell]^n$ and assuming that E is a CM curve. If E is a non-CM curve, it is still true by the theorems of Bachmakov (see [4] or [18, Chapter V, Theorem 5.2]).

In addition, the primes which ramify in the extension L/\mathbb{Q} are exactly those primes dividing $\ell\Delta_E$.

Now, fix a number field K_i with $1 \leq i \leq n$, note that every rational point P in $E(K_i)$ has a homogeneous coordinates of the form $[x, y, z]$ with $x, y, z \in O_{K_i}$ and at least one of x, y, z in $O_{K_i}^*$, where O_{K_i} is the ring of integers and $O_{K_i}^*$ is its group of units. Pick a prime $p \nmid \ell\Delta_E$ which splits completely in K , let \mathfrak{p}_i be a prime ideal of O_{K_i} above p . Then, the reduction map modulo \mathfrak{p}_i is defined by

$$E(K_i) \rightarrow E(O_{K_i}/\mathfrak{p}_i), \quad P = [x, y, z] \mapsto [x, y, z] \pmod{\mathfrak{p}_i}.$$

So, by the construction of K_i and noticing the choice of p , the equation

$$(3) \quad \ell X = P_i$$

has a solution in $E(\mathbb{F}_p)$, where X is an unknown, if and only if $[O_{K_i}/\mathfrak{p}_i : \mathbb{F}_p] = 1$, that is p splits completely in K_i .

In particular, if we indeed have some K_i such that $K_i \neq K$, then by the above discussion we can choose a conjugation class C in the Galois group $\text{Gal}(L/\mathbb{Q})$ such that each of its corresponding primes p is unramified in L/\mathbb{Q} , p is a prime of good reduction, every $\sigma \in C$ is the identity map when restricted to K , and p splits completely in some fields K_i but it does not split completely in the other fields K_j with $j \neq i$ (these corresponding fields must not be trivial extensions of K), which means that for some points P_i the equation (3) has a solution in $E(\mathbb{F}_p)$ but for the others there is no such solution.

2.5. The Chebotarev Density Theorem. For the convenience of the reader, we restate two useful results as follows. The first one is due to Hensel, see [28, Proposition 6]; while the second is about the least prime ideal in the Chebotarev Density Theorem, see [16, 17].

Lemma 10. *Let L/\mathbb{Q} be a Galois extension of degree n and ramified only at the primes p_1, \dots, p_m . Then, we have*

$$\log |D_L| \leq n \log n + n \sum_{i=1}^m \log p_i,$$

where D_L is the discriminant of L/\mathbb{Q} .

Lemma 11. *There exists an effectively computable positive absolute constant c_1 such that for any number field K , any finite Galois extension L/K and any conjugacy class C of $\text{Gal}(L/K)$, there exists a prime ideal \mathfrak{p} of K which is unramified in L , for which the Artin symbol $\left[\frac{L/K}{\mathfrak{p}} \right] = C$ and the norm $N_{K/\mathbb{Q}}(\mathfrak{p})$ is a rational prime, and which satisfies the bound*

$$N_{K/\mathbb{Q}}(\mathfrak{p}) \leq 2|D_L|^{c_1};$$

furthermore, under GRH, there is an effectively computable absolute constant c_2 such that

$$N_{K/\mathbb{Q}}(\mathfrak{p}) \leq c_2(\log |D_L|)^2.$$

3. THE EXISTENCE AND CONSTRUCTION OF x -PSEUDOLINEARLY DEPENDENT POINTS

3.1. Cases of existence and non-existence. Before proving our main results, we want to first consider the existence problem of pseudolinearly dependent points. In this section, E is a fixed elliptic curve of rank r over \mathbb{Q} , and Γ is a fixed subgroup of $E(\mathbb{Q})$ with rank s .

If the ranks of E and Γ satisfy $s < r$, then x -pseudolinearly dependent points of Γ do exist. Indeed, since $s < r$, we can take a point $R \in E(\mathbb{Q})$ of infinite order such that $\langle R \rangle \cap \Gamma = \{O_E\}$, where O_E is the point at infinity of E . Pick an arbitrary point $P \in \Gamma$, it is easy to see that the following point

$$(4) \quad Q = P + \text{lcm} \{ \#E(\mathbb{Q})_p / \#\Gamma_p : p \leq x \text{ of good reduction} \} R,$$

where, as usual, “lcm” means the least common multiple, is an x -pseudolinearly dependent point of Γ for any sufficiently large $x > 0$ (that is, there exists at least one prime of good reduction not greater than x).

In the construction (4), we can see that $\langle Q \rangle \cap \Gamma = \{O_E\}$. Actually, when x is sufficiently large, any x -pseudolinearly dependent point of Γ must satisfy this property.

Proposition 12. *There exists a sufficiently large constant M depending on E and Γ such that for any $x > M$, every x -pseudolinearly dependent point Q of Γ satisfies $\langle Q \rangle \cap \Gamma = \{O_E\}$.*

Proof. Consider the subgroup

$$\tilde{\Gamma} = \{P \in E(\mathbb{Q}) : mP \in \Gamma \text{ for some } m \in \mathbb{Z}\}.$$

Notice that $\tilde{\Gamma}$ is also a finitely generated group, and by construction each element in the quotient group $\tilde{\Gamma}/\Gamma$ is of finite order. So, $\tilde{\Gamma}/\Gamma$ is a finite group. Then, we let $n = [\tilde{\Gamma} : \Gamma]$ and assume that $\tilde{\Gamma}/\Gamma = \{P_0 = O_E, P_1, \dots, P_{n-1}\}$. If $n = 1$, then everything is done. Now, we assume that $n > 1$.

For any P_i , $1 \leq i \leq n-1$, since $P_i \notin \Gamma$, by Lemma 9 there exists a prime p_i of good reduction such that $P_i \notin \Gamma_{p_i}$. Then, we choose a constant, say M , such that $M \geq p_i$ for any $1 \leq i \leq n-1$. Thus, when $x > M$, any P_i ($1 \leq i \leq n-1$) is not an x -pseudolinearly dependent point of Γ , and then any point $P \in \tilde{\Gamma}$ is also not such a point. This in fact completes the proof. \square

The following result says that the case (that is $s < r$) in (4) is the only one meaningful case for x -pseudolinearly dependent points when x is sufficiently large.

Proposition 13. *If Γ is a full rank subgroup of $E(\mathbb{Q})$ (that is $s = r$), then there exists a constant M depending on E and Γ such that for any $x > M$, there is no x -pseudolinearly dependent point of Γ .*

Proof. Since Γ is of full rank, the index $[E(\mathbb{Q}) : \Gamma]$ is finite. Let $n = [E(\mathbb{Q}) : \Gamma]$. We can assume that $n > 1$. Now, we suppose that $E(\mathbb{Q})/\Gamma = \{P_0 = O_E, P_1, \dots, P_{n-1}\}$. So, $P_i \notin \Gamma$ for any $1 \leq i \leq n-1$.

For any P_i ($1 \leq i \leq n-1$), since $P_i \notin \Gamma$, by Lemma 9 there exists a prime p_i of good reduction such that $P_i \notin \Gamma_{p_i}$. Then, we choose a constant, say M , such that $M \geq p_i$ for any $1 \leq i \leq n-1$.

Pick an arbitrary point $Q \in E(\mathbb{Q}) \setminus \Gamma$, then there is exactly one P_i ($1 \leq i \leq n-1$) such that $Q - P_i \in \Gamma$. By the choice of p_i , we deduce that $Q \notin \Gamma_{p_i}$. Thus, Q is not an x -pseudolinearly dependent point of Γ for any $x > M$. \square

We remark that directly by Lemma 9, any given point in $E(\mathbb{Q})$ is not an x -pseudolinearly dependent point of Γ for x sufficiently large. Note that $E(\mathbb{Q})$ has finitely many torsion points, so by choosing large enough x , none of the torsion points in $E(\mathbb{Q})$ is an x -pseudolinearly dependent point of Γ .

As an example, we present the following explicit result. Note that by definition, if a point in $E(\mathbb{Q})$ is not an \mathbb{F}_p -pseudolinearly dependent point of Γ , then it is not an x -pseudolinearly dependent point of Γ for any $x \geq p$.

Proposition 14. *Suppose that $E(\mathbb{Q})$ is of rank 1 and $E(\mathbb{Q}) = \langle P \rangle$. Fix a prime p of good reduction, let m be a positive divisor of $\#E(\mathbb{Q})_p$, and set $\Gamma = \langle mP \rangle$. Then, there is no \mathbb{F}_p -pseudolinearly dependent point of Γ .*

Proof. If $m = 1$, then nothing needs to be done. Now we assume that $m > 1$.

Suppose that there exists a rational point $Q = nP \in E(\mathbb{Q})$ such that $Q \notin \Gamma$ but $Q \in \Gamma_p$, that is Q is an \mathbb{F}_p -pseudolinearly dependent point of Γ . Then, we have $m \nmid n$, and $Q \equiv kmP$ modulo p for some integer k . Thus, we have $(km - n)P \equiv O_E$ modulo p . Then, noticing the choice of m , we must have $m \mid (km - n)$, and so $m \mid n$. This leads to a contradiction. So, there is no such point Q , and the desired result follows. \square

3.2. Construction. In the sequel, E is a fixed elliptic curve of rank $r \geq 1$ over \mathbb{Q} , and Γ is a given subgroup of $E(\mathbb{Q})$ with rank $s < r$.

In order to get upper bounds on the height of pseudolinearly dependent points, the following construction is slightly different from what we give in Section 3.1.

For any prime p of good reduction related to E , we let

$$N_p = \#E(\mathbb{F}_p) \quad \text{and} \quad T_p = \#\Gamma_p,$$

and set $N_p = T_p = 1$ for all other primes p . Given a sufficiently large $x > 0$ (at least one prime of good reduction is not greater than x), we also define

$$L_x = \text{lcm} \{N_p/T_p : p \leq x\}.$$

Take a point $R \in E(\mathbb{Q})$ of infinite order such that $\langle R \rangle \cap \Gamma = \{O_E\}$, then pick an arbitrary point $P \in \Gamma$ and set

$$Q = P + L_x R.$$

It is easy to see that $Q \notin \Gamma$ but as a point in $E(\mathbb{F}_p)$, $Q \in \Gamma_p$ for every prime $p \leq x$ of good reduction.

Since the coordinates of points in $E(\mathbb{Q})$ are rational numbers, for any subset $S \subseteq E(\mathbb{Q})$ there exists a point with the smallest Weil height among all the points in S . So, noticing $s < r$, we choose a point with smallest Weil height in the subset consisting of non-torsion points R in $E(\mathbb{Q}) \setminus \Gamma$ with $\langle R \rangle \cap \Gamma = \{O_E\}$, we denote this point by R_{\min} . Thus, $\mathfrak{h}(R_{\min})$ is fixed if E and Γ are given.

Now, we define a point $Q_{\min} \in E(\mathbb{Q})$ as follows:

$$(5) \quad Q_{\min} = L_x R_{\min}.$$

As before, $Q_{\min} \notin \Gamma$ but $Q_{\min} \in \Gamma_p$ for every prime $p \leq x$ of good reduction. We also have

$$(6) \quad \hat{h}(Q_{\min}) = L_x^2 \hat{h}(R_{\min}) = L_x^2 (\mathfrak{h}(R_{\min}) + O(1)) \ll L_x^2,$$

which comes from the fact that $\mathfrak{h}(R_{\min})$ is fixed when E and Γ are given.

Finally, we want to give a trivial upper bound for $\hat{h}(Q_{\min})$, which can be viewed as a comparison of our main results.

Recalling the Hasse bound

$$|N_p - p - 1| \leq 2p^{1/2}$$

for any prime p of good reduction (see [29, Chapter V, Theorem 1.1]), we derive the inequality

$$\begin{aligned} \prod_{p \leq x} N_p &\leq \prod_{p \leq x} (p + 2p^{1/2} + 1) = \prod_{p \leq x} p(1 + p^{-1/2})^2 \\ &= \exp \left(\sum_{p \leq x} \log p + 2 \sum_{p \leq x} \log(1 + p^{-1/2}) \right) \\ (7) \quad &\leq \exp \left(\sum_{p \leq x} \log p + 2 \sum_{p \leq x} p^{-1/2} \right) \\ &= \exp(O(\sqrt{x}/\log x)) \prod_{p \leq x} p. \end{aligned}$$

Now using the prime number theorem with the currently best known error term:

$$(8) \quad \sum_{p \leq x} \log p = x + O\left(x \exp\left(-c(\log x)^{3/5}(\log \log x)^{-1/5}\right)\right)$$

with $x \geq 3$ and some absolute constant $c > 0$, see [11, Corollary 8.30], we obtain

$$(9) \quad \prod_{p \leq x} N_p \leq \exp\left(x + O\left(x \exp\left(-c(\log x)^{3/5}(\log \log x)^{-1/5}\right)\right)\right).$$

Combining (9) with (6), we derive the following trivial upper bound for $\hat{h}(Q_{\min})$:

$$(10) \quad \begin{aligned} \hat{h}(Q_{\min}) &\ll L_x^2 \leq \prod_{p \leq x} N_p^2 \\ &\leq \exp\left(2x + O\left(x \exp\left(-c(\log x)^{3/5}(\log \log x)^{-1/5}\right)\right)\right). \end{aligned}$$

Next, we give some better upper bounds for $\hat{h}(Q_{\min})$, which automatically provide proofs of our main theorems on the upper bounds.

4. PROOFS OF UPPER BOUNDS: THEOREMS 4, 5 AND 6

As mentioned above, to achieve our purpose, it suffices to bound the canonical height of Q_{\min} , given by (5), that is, $\hat{h}(Q_{\min})$.

Here, we also use the notation and some results of Section 3.2, in particular, the bound (6).

By definition, we get

$$L_x \leq \prod_{p \leq x} N_p / T_p.$$

Our approach is to get upper and lower bounds for

$$\prod_{p \leq x} N_p \quad \text{and} \quad \prod_{p \leq x} T_p,$$

respectively.

We also need the following result from [1, Proposition 5.4] (see [10, Lemma 14] for a previous result).

Lemma 15. *For any real $z > 1$, we have*

$$\#\{p : T_p < z\} \ll z^{1+2/s} / \log z.$$

4.1. Proof of Theorem 4. Since Γ has rank zero, by the injectivity of the reduction map restricted to the torsion subgroup, we can see that $T_p = \#\Gamma$ for any prime p of good reduction.

We also recall the prime number theorem in the following simplified form

$$(11) \quad \pi(x) = \frac{x}{\log x} + O(x/(\log x)^2),$$

which follows immediately from (8).

Now, using (9) and (11) we have

$$\begin{aligned} L_x &\leq (\#\Gamma)^{-\pi(x)} \prod_{p \leq x} N_p \\ &\leq \exp \left(x - \log(\#\Gamma) \frac{x}{\log x} + O(x/(\log x)^2) \right). \end{aligned}$$

From (6) we conclude that for a sufficiently large $x > 0$, we have

$$\hat{h}(Q_{\min}) \leq \exp \left(2x - 2 \log(\#\Gamma) \frac{x}{\log x} + O(x/(\log x)^2) \right),$$

which completes the proof.

4.2. Proof of Theorem 5. The desired result follows from the following estimate on the canonical height of Q_{\min} .

Lemma 16. *If $s \geq 1$, then for a sufficiently large $x > 0$, we have*

$$\hat{h}(Q_{\min}) \leq \exp \left(\frac{4}{s+2} x + O(x/\log x) \right).$$

Proof. For a sufficiently large x , we define

$$J = \left\lfloor \frac{s}{s+2} \log x \right\rfloor \geq 1 \quad \text{and} \quad Z_j = x^{s/(s+2)} e^{-j}, \quad j = 0, \dots, J.$$

Here e is the base of the natural logarithm. Note that $1 \leq Z_J < e$.

Since $s \geq 1$, the number of primes p such that $T_p = 1$ or 2 is finite; we denote this number by N , which depends only on Γ . Let N_0 be the number of primes $p \leq x$ with $T_p \geq Z_0$. Furthermore, for $j = 1, \dots, J$ we define N_j as the number of primes $p \leq x$ with $Z_{j-1} > T_p \geq Z_j$. Clearly

$$N + \sum_{j=0}^J N_j \geq \pi(x).$$

So, noticing $Z_0 = x^{s/(s+2)}$ we now derive

$$\prod_{p \leq x} T_p \geq \prod_{j=0}^J Z_j^{N_j} \geq Z_0^{\pi(x)-N} \prod_{j=0}^J e^{-jN_j} = Z_0^{\pi(x)-N} \exp(-\Lambda),$$

where

$$\Lambda = \sum_{j=1}^J jN_j.$$

Recalling the definition of Z_0 , and using (11), we obtain

$$(12) \quad \prod_{p \leq x} T_p \geq \exp \left(\frac{s}{s+2}x - \Lambda + O(x/\log x) \right).$$

To estimate Λ , we note that by Lemma 15, for any positive integer $I \leq J$ we have

$$\sum_{j=I}^J N_j \leq \#\{p : T_p < Z_0 e^{-I+1}\} \ll \frac{(Z_0 e^{-I+1})^{1+2/s}}{\log Z_0 - I + 1}.$$

Thus for $I \leq J/2$, noticing $J \leq \log Z_0$ we obtain

$$(13) \quad \sum_{j=I}^J N_j \ll \frac{(Z_0 e^{-I})^{1+2/s}}{\log Z_0} \ll e^{-I(1+2/s)} \frac{x}{\log x},$$

while for any $J/2 < I \leq J$ we use the bound

$$(14) \quad \sum_{j=I}^J N_j \ll (Z_0 e^{-I+1})^{1+2/s} \ll (\sqrt{Z_0})^{1+2/s} = x^{1/2}.$$

Hence, via partial summation, combining (13) and (14), we derive

$$\begin{aligned} \Lambda &= \sum_{I=1}^J \sum_{j=I}^J N_j \ll \frac{x}{\log x} \sum_{1 \leq I \leq J/2} e^{-I(1+2/s)} + x^{1/2} \sum_{J/2 < I \leq J} 1 \\ &\ll \frac{x}{\log x} + Jx^{1/2} \ll \frac{x}{\log x}. \end{aligned}$$

This bound on Λ , together with (12), implies

$$\prod_{p \leq x} T_p \geq \exp \left(\frac{s}{s+2}x + O(x/\log x) \right).$$

Therefore using (9), we obtain

$$L_x \leq \prod_{p \leq x} N_p/T_p \leq \exp \left(\frac{2}{s+2}x + O(x/\log x) \right).$$

Therefore, the desired result follows from the bound (6). \square

4.3. Proof of Theorem 6. We first restate two general results from [1, Theorems 1.2 and 1.4] in a form convenient for our applications.

Lemma 17. *Assume that E is a non-CM curve and $s \geq 19$. Under GRH, for $x \geq 2$ we have*

$$\#\{p \leq x : T_p < p/(\log p)^2\} \ll x/(\log x)^2.$$

Proof. Since there are only finitely many primes which do not yield good reductions related to E , we can only consider primes p of good reduction (that is $p \nmid \Delta_E$). Here, we directly use the notation and follow the arguments in the proof of [1, Theorem 1.2, Part (a)], where we choose the function $f(x)$ as $f(x) = (\log x)^2$. Let \mathcal{B}_1 and \mathcal{B}_2 be two sets defined in [1] such that

$$\#\{p \leq x : p \nmid \Delta_E, T_p < p/(\log p)^2\} \leq \#\mathcal{B}_1 + \#\mathcal{B}_2 + O(x/(\log x)^2),$$

where $O(x/(\log x)^2)$ comes from $\pi(x/\log x) = O(x/(\log x)^2)$. In particular, we have

$$\#\mathcal{B}_1 \ll \frac{x}{(\log x)^{(s+2)/s} \cdot (s(s+2)^{-1} \log x - \log \log x)}$$

and

$$\#\mathcal{B}_2 \ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\left(x^{1/2+\alpha+(5+\alpha/2) \cdot (2/(s+2)+\alpha)}\right),$$

where $g(x) = f(x/\log x)/3$, and the positive real number α is chosen such that

$$\frac{1}{2} + \alpha + \left(5 + \frac{\alpha}{2}\right) \cdot \left(\frac{2}{s+2} + \alpha\right) < 1,$$

which at least requires that $1/2 + 6\alpha < 1$, that is $\alpha < 1/12$. Note that such α indeed exists because $s \geq 19$.

It is easy to see that

$$\#\mathcal{B}_1 \ll x/(\log x)^2 \quad \text{and} \quad \#\mathcal{B}_2 \ll x/(\log x)^2,$$

where the second upper bound comes from $2(1-\alpha) > 1$. Collecting these estimates, we get the required upper bound. \square

Lemma 18. *Assume that E is a CM curve and $s \geq 7$. Under GRH, for $x \geq 2$ we have*

$$\#\{p \leq x : T_p < p/(\log p)^2\} \ll x/(\log x)^2.$$

Proof. The proof here almost follows the arguments in the proof of [1, Theorem 1.4] only with a few minor changes, where as in Lemma 17 we again choose the function $f(x)$ as $f(x) = (\log x)^2$. For any prime p of good reduction, let $i_p = [E(\mathbb{F}_p) : \Gamma_p]$. The following can be derived from [1]:

$$\#\{p \leq x : p \nmid \Delta_E, T_p < p/(\log p)^2\} \leq \#\tilde{\mathcal{B}}_1 + \#\tilde{\mathcal{B}}_2 + O(x/(\log x)^2),$$

where

$$\tilde{\mathcal{B}}_1 = \{p \leq x : p \nmid \Delta_E, i_p \in (x^\kappa, 3x]\},$$

$$\tilde{\mathcal{B}}_2 = \{p \leq x : p \nmid m\Delta_E, m \mid i_p, \text{ for some } m \in (g(x), x^\kappa]\}$$

with $g(x) = f(x/\log x)/3$ and some real number $\kappa > 0$ to be chosen later on.

Applying Lemma 15, we have

$$\begin{aligned} \#\tilde{\mathcal{B}}_1 &= \#\{p \leq x : p \nmid \Delta_E, T_p < N_p/x^\kappa\} \\ &\leq \#\{p \leq x : p \nmid \Delta_E, T_p < 3x^{1-\kappa}\} \ll \frac{x^{(1-\kappa)(s+2)/s}}{(1-\kappa)\log x}. \end{aligned}$$

For any positive integer m , let $\omega(m)$ and $d(m)$ denote, respectively, the number of distinct prime divisors of m and the number of positive integer divisors of m .

Now, $\#\tilde{\mathcal{B}}_2$ can be estimated as in [1] as follows:

$$\#\tilde{\mathcal{B}}_2 \ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\left(x^{1/2} \log x \cdot \sum_{1 \leq m \leq x^\kappa} m a^{\omega(m)/2} d(m)\right).$$

where a is the absolute constant of [1, Proposition 6.7]. Now, using [1, Equation (6.21)] we obtain

$$\begin{aligned} \#\tilde{\mathcal{B}}_2 &\ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\left(x^{1/2+2\kappa} (\log x)^{1+\beta}\right) \\ &\ll \frac{x}{(\log x)^2} + O\left(x^{1/2+2\kappa} (\log x)^{1+\beta}\right), \end{aligned}$$

where α is an arbitrary real number in the interval $(0, 1)$ such that $2(1-\alpha) > 1$, and $\beta > 2$ is some positive integer.

Moreover, we choose the real number κ such that

$$(1-\kappa)(s+2)/s < 1 \quad \text{and} \quad \frac{1}{2} + 2\kappa < 1.$$

Thus, we get

$$(15) \quad \frac{2}{s+2} < \kappa < \frac{1}{4}.$$

Since $s \geq 7$, such real number κ indeed exists.

Therefore, for any fixed real number κ satisfying (15) (for example, $\kappa = 11/45$) we obtain

$$\#\{p \leq x : p \nmid \Delta_E, T_p < p/(\log p)^2\} \ll x/(\log x)^2,$$

which completes the proof of this lemma. \square

Finally, the following estimate completes our proof.

Lemma 19. *Suppose that either $s \geq 19$ if E is a non-CM curve, or $s \geq 7$ if E is a CM curve. Under GRH, for a sufficiently large $x > 0$, we have*

$$\hat{h}(Q_{\min}) \leq \exp(4x(\log \log x)/\log x + O(x/\log x)).$$

Proof. First, we have

$$\begin{aligned} \prod_{p \leq x} T_p &\geq \prod_{\substack{p \leq x \\ T_p \geq p/(\log p)^2}} \frac{p}{(\log p)^2} \cdot \prod_{\substack{p \leq x \\ T_p < p/(\log p)^2}} T_p \\ &= \prod_{p \leq x} \frac{p}{(\log p)^2} \prod_{\substack{p \leq x \\ T_p < p/(\log p)^2}} \frac{T_p (\log p)^2}{p}. \end{aligned}$$

Using the trivial lower bound $T_p \geq 1$ and Lemma 17 and Lemma 18, we derive

$$\begin{aligned} \prod_{p \leq x} T_p &\geq \prod_{p \leq x} p \cdot \prod_{p \leq x} (\log p)^{-2} \cdot \prod_{\substack{p \leq x \\ T_p < p/(\log p)^2}} (\log p)^2/p \\ &\geq \left(\frac{(\log x)^2}{x} \right)^{O(x/(\log x)^2)} \prod_{p \leq x} p \cdot \prod_{p \leq x} (\log p)^{-2}, \end{aligned}$$

where the last inequality follows from Lemma 17 and Lemma 18.

Thus, using (7), we obtain

$$\begin{aligned} L_x &\leq \prod_{p \leq x} N_p/T_p \leq \exp(O(x/\log x)) \prod_{p \leq x} (\log p)^2 \\ &\leq \exp\left(2 \frac{x \log \log x}{\log x} + O(x/\log x)\right), \end{aligned}$$

where the last inequality is derived from (11) and the trivial estimate

$$\sum_{p \leq x} \log \log p \leq \pi(x) \log \log x.$$

Therefore, the desired result follows from the bound $\hat{h}(Q_{\min}) \ll L_x^2$. \square

5. PROOFS OF LOWER BOUNDS: THEOREMS 7 AND 8

5.1. Proof of Theorem 7. Now, assume that Γ is a torsion subgroup of $E(\mathbb{Q})$, and let $Q \in E(\mathbb{Q})$ be an x -pseudolinearly dependent point of Γ for a sufficiently large x . Let m be the number of primes of bad reduction. Then, since $Q \in \Gamma_p$ for any prime $p \leq x$ of good reduction, there exists a rational point $P \in \Gamma$ such that at least $(\pi(x) - m)/\#\Gamma$ primes $p \leq x$ of good reduction let the point $Q - P$ become the point at infinity modulo p . In view of (1), this implies that

$$\begin{aligned} \mathfrak{h}(Q - P) &\geq 2 \log \prod_{p \leq (\pi(x) - m)/\#\Gamma} p \\ &\geq \frac{2}{\#\Gamma} x / \log x + O(x/(\log x)^2), \end{aligned}$$

where the last inequality follows from (8) and (11). Note that P is a torsion point, then using [29, Chapter VIII, Theorem 9.3] we obtain

$$\begin{aligned} \hat{h}(Q) &= \hat{h}(Q) + \hat{h}(P) = \frac{1}{2} \left(\hat{h}(Q + P) + \hat{h}(Q - P) \right) \\ (16) \quad &\geq \frac{1}{2} \hat{h}(Q - P) \geq \frac{1}{2} \mathfrak{h}(Q - P) + O(1) \\ &\geq \frac{1}{\#\Gamma} x / \log x + O(x/(\log x)^2), \end{aligned}$$

which gives the claimed lower bound for the height of the point Q .

5.2. Proof of Theorem 8. Here, we assume that Γ is a free subgroup of rank s generated by P_1, P_2, \dots, P_s . This assumption comes from the discussions in Section 2.4.

We first prove a result, which can be viewed as an effective version of Lemma 9 in some sense.

Lemma 20. *Let $Q \in E(\mathbb{Q}) \setminus \Gamma$ be a point of infinite order such that $\langle Q \rangle \cap \Gamma = \{O_E\}$. Then, there exists a prime p of good reduction satisfying*

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log \log \hat{h}(Q)$$

such that $Q \notin \Gamma_p$. If furthermore assuming GRH, we even have

$$p \ll (\log \hat{h}(Q))^{4s+12} (\log \log \hat{h}(Q))^2.$$

Proof. Let Q_1, Q_2, \dots, Q_r be a fixed basis of the free part of $E(\mathbb{Q})$. Since the point Q is of infinite order, it can be represented as

$$Q = Q_0 + m_1 Q_1 + m_2 Q_2 + \dots + m_r Q_r,$$

where Q_0 is a torsion point of $E(\mathbb{Q})$, and there is at least one $m_i \neq 0$ ($1 \leq i \leq r$). By [29, Chapter IX, Exercise 9.8 (e)], we immediately have

$$\hat{h}(Q - Q_0) \gg \max_{1 \leq i \leq r} m_i^2.$$

Noticing that Q_0 is a torsion point, as (16) we obtain

$$(17) \quad \hat{h}(Q) \geq \frac{1}{2} \hat{h}(Q - Q_0) \gg \max_{1 \leq i \leq r} m_i^2.$$

Now, take any $m_i \neq 0$ and let ℓ be the smallest prime such that $\ell \nmid m_i$. Since the number $\omega(m)$ of distinct prime factors of an integer $m \geq 2$ satisfies

$$\omega(m) \ll \frac{\log m}{\log \log m}$$

(because we obviously have $\omega(m)! \leq m$), using the prime number theorem we get

$$\ell \ll \log |m_i|,$$

which together with (17) yields that

$$(18) \quad \ell \ll \log \hat{h}(Q).$$

By the choice of ℓ , we see that there is no point $R \in E(\mathbb{Q})$ such that $Q = \ell R$. This implies that the number field $\mathbb{Q}(E[\ell], \ell^{-1}Q)$ is not a trivial extension of $\mathbb{Q}(E[\ell])$. Consider the number field

$$L = \mathbb{Q}(E[\ell], \ell^{-1}Q, \ell^{-1}P_1, \dots, \ell^{-1}P_s),$$

and set $K = \mathbb{Q}(E[\ell])$. By the discussions in Section 2.4, we can choose a conjugation class C in the Galois group $\text{Gal}(L/\mathbb{Q})$ such that each of its corresponding primes p is unramified in L/\mathbb{Q} , p is a prime of good reduction, every $\sigma \in C$ is the identity map when restricted to K , and especially each equation $\ell X = P_i$ has solution in $E(\mathbb{F}_p)$ for $1 \leq i \leq s$ but the equation $\ell X = Q$ has no such solution, which implies that

$$Q \notin \Gamma_p.$$

By Lemma 11, we can choose such a prime p such that

$$(19) \quad \log p \ll \log |D_L|;$$

if under GRH, we even have

$$(20) \quad p \ll (\log |D_L|)^2.$$

From Lemma 10 and noticing that only the primes dividing $\ell \Delta_E$ ramify in L , we get

$$(21) \quad \log |D_L| \leq n \log n + n \log(\ell \Delta_E) \ll n \log n + n \log \ell,$$

where $n = [L : \mathbb{Q}]$. Using (2), we obtain

$$(22) \quad n \leq \ell^{2s+6}.$$

Combining (18), (19), (20), (21) with (22), we unconditionally have

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log \log \hat{h}(Q),$$

and conditionally we have

$$p \ll (\log \hat{h}(Q))^{4s+12} (\log \log \hat{h}(Q))^2,$$

which concludes the proof. \square

Now, we are ready to prove Theorem 8.

For a sufficiently large x , by Proposition 12, any x -pseudolinearly dependent point Q of Γ satisfies $\langle Q \rangle \cap \Gamma = \{O_E\}$. Then from Lemma 20, there is an unconditional prime p of good reduction satisfying

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log \log \hat{h}(Q)$$

such that $Q \notin \Gamma_p$. Since $x < p$ by definition, we obtain

$$\log x \ll (\log \hat{h}(Q))^{2s+6} \log \log \hat{h}(Q),$$

which implies that

$$\hat{h}(Q) \geq \exp((\log x)^{1/(2s+6)+o(1)}).$$

Similarly, if assuming GRH, we can obtain

$$\hat{h}(Q) \geq \exp(x^{1/(4s+12)+o(1)}),$$

which completes the proof.

6. COMMENTS

We remark that the upper bound of Theorem 4 is only slightly better than the trivial bound (10), although the ratio between the two estimates tends to zero whenever $\#\Gamma > 1$.

In Section 5, we get some partial results on the lower bound for the height of x -pseudolinearly dependent points. In fact, the height of such points certainly tends to infinity as $x \rightarrow +\infty$.

Indeed, let E be an elliptic curve over \mathbb{Q} of rank $r \geq 1$, and let Γ be a subgroup of $E(\mathbb{Q})$ with rank $s < r$. We have known that for any sufficiently large x , there exist infinitely many x -pseudolinearly dependent points of Γ . For any $x > 0$, if such points exist, as before we can choose a point, denoted by Q_x , with smallest Weil height among all these points; otherwise if there are no such points, we let $Q_x = O_E$. Thus, we get a subset $S = \{Q_x : x > 0\}$ of $E(\mathbb{Q})$, and for any $x < y$ we have $\mathfrak{h}(Q_x) \leq \mathfrak{h}(Q_y)$. By Lemma 9, we know that for any fixed point

$Q \in E(\mathbb{Q})$, it can not be an x -pseudolinearly dependent point of Γ for any sufficiently large x . So, S is an infinite set. Since it is well-known that there are only finitely many rational points of $E(\mathbb{Q})$ with bounded height, we obtain

$$\lim_{x \rightarrow +\infty} \mathfrak{h}(Q_x) = +\infty,$$

which implies that $\lim_{x \rightarrow +\infty} \hat{h}(Q_x) = +\infty$. This immediately implies that for the point Q_{\min} constructed in Section 3.2, its height $\hat{h}(Q_{\min})$ also tends to infinity as $x \rightarrow +\infty$. Moreover, let p_n denote the n th prime, that is $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \dots$. For any $n \geq 1$, denote by T_n the set of p_n -pseudolinearly dependent points of Γ . Obviously, $T_{n+1} \subseteq T_n$ and $\mathfrak{h}(Q_{p_{n+1}}) \geq \mathfrak{h}(Q_{p_n})$ for any $n \geq 1$. For any sufficiently large n , we conjecture that $T_{n+1} \subsetneq T_n$. If furthermore one could prove that $\mathfrak{h}(Q_{p_{n+1}}) > \mathfrak{h}(Q_{p_n})$ for any sufficiently large n , this would lead to a lower bound of the form

$$\mathfrak{h}(Q_x) \geq \log x + O(\log \log x),$$

as the values of $\mathfrak{h}(Q_x)$ are logarithms of integer numbers and there are about $x/\log x$ primes not greater than x .

In Lemma 20, if we choose Γ as a torsion subgroup, we can also get a similar unconditional upper bound. Indeed, for a prime p of good reduction, suppose that $Q \in \Gamma_p$. Then, $Q - P \equiv O_E$ modulo p for some $P \in \Gamma$. According to (1), we have $p \leq \exp(0.5\mathfrak{h}(Q - P))$. Since P is a torsion point, as (16) we get $p \leq \exp(\hat{h}(Q) + O(1))$. Thus, we can choose a prime p of good reduction satisfying

$$p \leq \exp(\hat{h}(Q) + O(1))$$

such that $Q \notin \Gamma_p$.

Finally, we want to remark that the definition of pseudolinearly dependent point can be generalized to many settings where there exist reduction maps modulo “primes” (which can be prime numbers, prime ideals, monic irreducible polynomials, and so on), such as number fields, function fields, curves of higher genus, Abelian varieties, and so on.

ACKNOWLEDGEMENT

The authors would like to thank Wojciech Gajda for very stimulating discussions which led to the idea of this work and also for his valuable comments on an early version of the paper. These discussions took place at the Max Planck Institute for Mathematics, Bonn, whose support and hospitality are gratefully acknowledged.

This work was also supported in part by the Australian Research Council Grants DP130100237 and DP140100118.

REFERENCES

- [1] A. Akbary, D. Ghioca and V. K. Murty, ‘Reductions of points on elliptic curves’, *Math. Ann.* **347** (2010), 365–394.
- [2] A. Akbary and V. K. Murty, ‘Reduction mod p of subgroups of the Mordell-Weil group of an elliptic curve’, *Int. J. Number Theory* **5** (2009), 465–487.
- [3] E. Bach, R. Lukes, J. Shallit and H. C. Williams, ‘Results and estimates on pseudopowers’, *Math. Comp.* **65** (1996), 1737–1747.
- [4] M. Bachmakov, ‘Un théorème de finitude sur la cohomologie des courbes elliptiques’, *C. R. Acad. Sci. Paris Sér. A-B* **270** (1970), A999–A1001.
- [5] G. Banaszak, ‘On a Hasse principle for Mordell-Weil groups’, *C. R. Math. Acad. Sci. Paris* **347** (2009), 709–714.
- [6] G. Banaszak, W. Gajda and P. Krasoń, ‘Detecting linear dependence by reduction maps’, *J. Number Theory* **115** (2005), 322–342.
- [7] G. Banaszak and P. Krasoń, ‘On arithmetic in Mordell-Weil groups’, *Acta Arith.* **150** (2011), 315–337.
- [8] J. Bourgain, S. Konyagin, C. Pomerance and I. E. Shparlinski, ‘On the smallest pseudopower’, *Acta Arith.* **140** (2009), 43–55.
- [9] W. Gajda and K. Górniewicz, ‘Linear dependence in Mordell-Weil groups’, *J. reine angew. Math.* **630** (2009), 219–233.
- [10] R. Gupta and M. R. Murty, ‘Primitive points on elliptic curves’, *Compos. Math.* **58** (1986), 13–44.
- [11] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
- [12] P. Jossen, ‘Detecting linear dependence on an abelian variety via reduction maps’, *Comment. Math. Helv.* **88**(2) (2013), 323–352.
- [13] P. Jossen and A. Perucca, ‘A counterexample to the local-global principle of linear dependence for Abelian varieties’, *C. R. Acad. Sci. Paris, Ser. I* **348** (2010), 9–10.
- [14] S. V. Konyagin, C. Pomerance, and I. E. Shparlinski, ‘On the distribution of pseudopowers’, *Canad. J. Math.* **62** (2010), 582–594.
- [15] E. Kowalski, ‘Some local-global applications of Kummer theory’, *Manuscripta Math.* **111** (2003), 105–139.
- [16] J. C. Lagarias and A. M. Odlyzko, ‘Effective versions of the Chebotarev density theorem’, *Algebraic Number Fields* (A. Fröhlich ed.), Academic Press, London, 1977, 409–464.
- [17] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, ‘A bound for the least prime ideal in the Chebotarev density theorem’, *Invent. Math.* **54** (1979), 271–296.
- [18] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer, Berlin, 1978.
- [19] S. Lang and H. Trotter, ‘Primitive points on elliptic curves’, *Bull. Amer. Math. Soc.* **83** (1977), 289–292.
- [20] A. Perucca, ‘On the problem of detecting linear dependence for products of abelian varieties and tori’, *Acta Arith.* **142** (2010), 119–128.
- [21] C. Pomerance and I. E. Shparlinski, ‘On pseudosquares and pseudopowers’, *Combinatorial Number Theory, Proc. of Integers Conf. 2007*, Walter de Gruyter, Berlin, 2009, 171–184.
- [22] K. Ribet, ‘Dividing rational points on abelian varieties of CM type’, *Compos. Math.* **33** (1976), 69–74.

- [23] M. Sadek, ‘On dependence of rational points on elliptic curves’, *C. R. Math. Rep. Acad. Sci. Canada* **38** (2016), 75–84.
- [24] A. Schinzel, ‘On the congruence $a^x \equiv b \pmod{p}$ ’, *Bull. Acad. Polon. Sci., Sér. Sci. Math. Astronom. Phys.* **8** (1960), 307–309.
- [25] A. Schinzel, ‘A refinement of a theorem of Gerst on power residues’, *Acta Arith.* **17** (1970), 161–168.
- [26] A. Schinzel, ‘On power residues and exponential congruences’, *Acta Arith.* **27** (1975), 397–420.
- [27] A. Schinzel, ‘On pseudosquares’, *New trends in probability and statistics, Palonga, 1996*, Vol. 4, 213–220, VSP, Utrecht, 1997.
- [28] J.-P. Serre, ‘Quelques applications du théorème de densité de Chebotarev’ *Publ. Math. IHES* **54** (1981), 323–401.
- [29] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Springer, Dordrecht, 2009.
- [30] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, Berlin, 1992.
- [31] T. Weston, ‘Kummer theory of abelian varieties and reduction of Mordell-Weil groups’, *Acta Arith.* **110** (2003), 77–88.

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY NSW 2052, AUSTRALIA

E-mail address: `shamin2010@gmail.com`

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY NSW 2052, AUSTRALIA

E-mail address: `igor.shparlinski@unsw.edu.au`